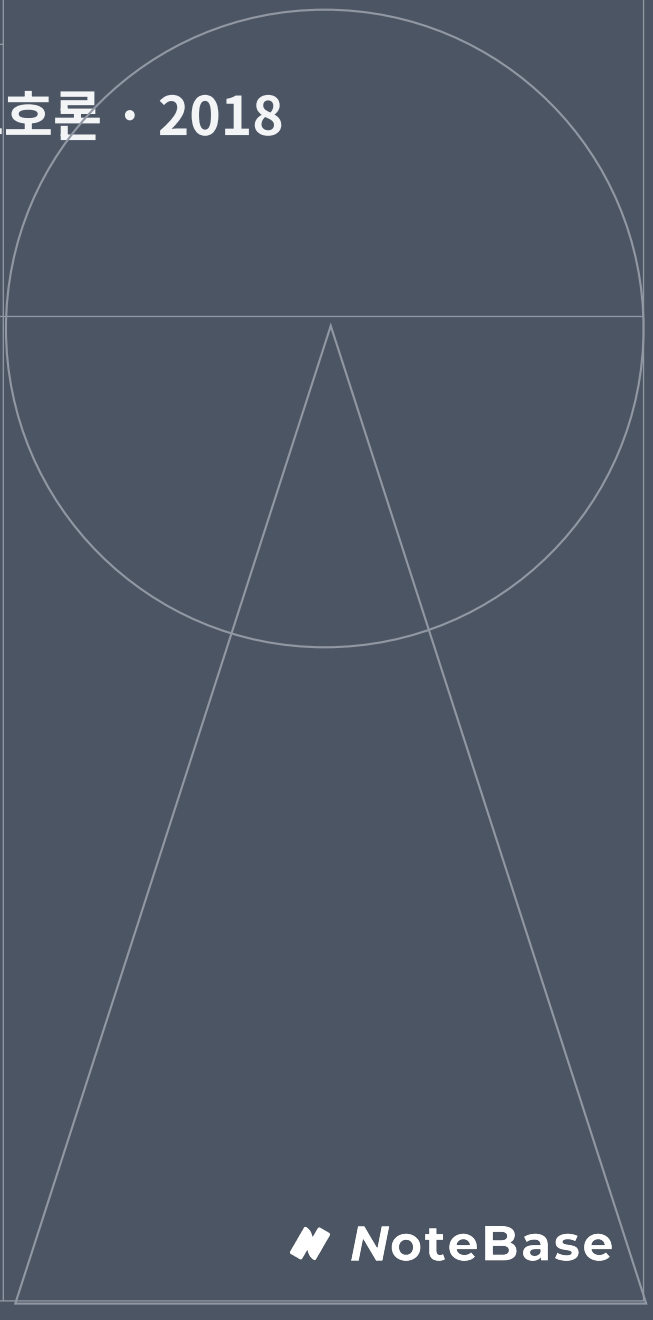
기출OX 해설집

공무원/지방직/9급 · 정보보호론 · 2018



NoteBase

기출OX 해설집

공무원/지방직/9급 · 정보보호론 · 2018

공무원/지방직/9급 · 정보보호론 · 2018

문 1. 정보보호의 3대 요소 중 가용성에 대한 설명으로 옳은 것은?

① 권한이 없는 사람은 정보자산에 대한 수정이 허락되지 않음을 의미한다.

② 권한이 없는 사람은 정보자산에 대한 접근이 허락되지 않음을 의미한다.

③ 정보를 암호화하여 저장하면 가용성이 보장된다.

④ DoS(Denial of Service) 공격은 가용성을 위협한다.

정답 4번

간단한 해설

가용성은 권한 있는 사용자가 **필요할 때 정보와 서비스를 이용할 수 있는 성질**이다. DoS 공격은 정상적인 서비스 이용을 방해하므로 가용성을 위협한다.

선지별 해설

① X: 권한 없는 사람의 수정을 막는 것은 가용성이 아니라 **무결성**에 대한 설명이다. 무결성은 정보가 허가 없이 변경되거나 훼손되지 않도록 하여 정확성과 완전성을 유지하는 성질이다.

② X: 권한 없는 사람의 정보 접근을 막는 것은 가용성이 아니라 **기밀성**에 대한 설명이다. 기밀성은 정보를 허가된 대상만 알 수 있도록 보호하는 성질이며, 가용성은 권한 있는 사용자가 필요할 때 정보를 이용할 수 있는지에 초점을 둔다.

③ X: 정보를 암호화하여 저장하는 것은 주로 **기밀성을 보호**하는 수단이다. 암호문은 적절한 복호화 키 없이 내용을 알아보기 어렵게 하지만, 서버 장애나 서비스 중단까지 막아 주지는 않으므로 암호화만으로 가용성이 보장되지는 않는다.

④ O: 가용성은 권한 있는 사용자가 필요할 때 정보와 서비스를 정상적으로 이용할 수 있는 성질이다. DoS(Denial of Service, 서비스 거부) 공격은 과도한 요청으로 자원을 소모시키는 등의 방법으로 **정상적인 서비스 이용을 방해**하므로 가용성을 위협한다.

NoteBase

문 2. ISO/IEC 27001에서 제시된 정보보안관리를 위한 PDCA 모델에서 ISMS의 지속적 개선을 위해 시정 및 예방 조치를 하는 단계는?

① Plan

② Do

③ Check

④ Act

정답 4번

간단한 해설

시정 및 예방 조치는 점검에서 얻은 결과를 바탕으로 정보보호관리체계(ISMS)를 **유지·개선하는 Act 단계**에서 수행한다. 문제를 확인하는 데서 나아가 원인을 제거하고 관리체계를 개선하는 활동이다.

공통 해설

PDCA 모델에서 Act는 정보보호관리체계(ISMS)를 유지·개선하는 단계이다. 내부감사와 경영검토 등의 결과를 바탕으로 **시정 및 예방 조치를 수행**하여 관리체계의 효과성을 지속적으로 높인다. 시정 조치는 발견된 부적합의 원인을 제거하여 재발을 막고, 예방 조치는 잠재적 부적합의 원인을 제거하여 발생을 막는다.

문항의 핵심은 계획 수립이나 계획의 실행, 결과 점검을 넘어 그 결과를 개선 조치로 연결한다는 데 있다. 특히 **Check는 운영 결과를 점검·평가**하는 단계이고, **Act는 점검 결과에 따라 개선**하는 단계이므로 구별해야 한다.

NoteBase

문 3. 보안 관리 대상에 대한 설명으로 ㉠~㉢에 들어갈 용어는?

○ (㉠) - 시스템과 네트워크의 접근 및 사용 등에 관한 중요 내용이 기록되는 것을 말한다.
○ (㉡) - 사용자와 시스템 또는 두 시스템 간의 활성화된 접속을 말한다.
○ (㉢) - 자산에 손실을 초래할 수 있는 원치 않는 사건의 잠재적 원인이나 행위자를 말한다.

① ㉠: 로그, ㉡: 세션, ㉢: 위험
② ㉠: 로그, ㉡: 세션, ㉢: 위협
③ ㉠: 백업, ㉡: 쿠키, ㉢: 위험
④ ㉠: 백업, ㉡: 쿠키, ㉢: 위협

정답 2번

간단한 해설

자산에 손실을 일으킬 수 있는 잠재적 원인이나 행위자는 **위협**이다. 위험은 그 위협으로 손실이 발생할 가능성과 영향을 함께 고려하는 개념이다.

빈칸별 해설

㉠ 로그: 시스템과 네트워크의 **접근·사용 이력을 기록**한 것이다. 예를 들어 로그인 시각과 접속 계정 등을 남겨 사후에 어떤 활동이 있었는지 확인한다. 백업은 데이터가 손상되거나 사라질 때 복구할 수 있도록 사본을 만들어 두는 것이므로, 활동 이력을 뜻하는 이 설명과 구별된다.

㉡ 세션: 사용자와 시스템 또는 두 시스템 사이에 유지되는 **활성화된 접속**이다. 쿠키는 웹사이트가 브라우저에 저장하도록 하는 데이터로, 세션을 식별하는 정보를 담을 수 있지만 접속 자체를 뜻하지는 않는다.

㉢ 위협: 자산에 손실을 초래할 수 있는 사건의 **잠재적 원인이나 행위자**이다. 공격자나 악성코드 등이 그 예이다. 위험은 위협이 실제로 자산에 피해를 줄 가능성과 그 피해의 크기를 고려하는 개념이므로, 손실의 원인이나 행위자 자체를 가리키는 위협과 구별된다.

㉠ 로그, ㉡ 세션, ㉢ 위협의 조합은 ②에 해당한다.

NoteBase

문 4. 유닉스 시스템에서 파일의 접근모드 변경에 사용되는 심볼릭 모드 명령어에 대한 설명으로 옳은 것은?

① chmod u-w: 소유자에게 쓰기 권한 추가

② chmod g+wx: 그룹, 기타 사용자에게 쓰기와 실행 권한 추가

③ chmod a+r: 소유자, 그룹, 기타 사용자에게 읽기 권한 추가

④ chmod o-w: 기타 사용자에게 쓰기 권한 추가

정답 3번

간단한 해설

chmod a+r에서 **a는 소유자·그룹·기타 사용자 모두**를, **+r은 읽기 권한 추가**를 뜻한다. 따라서 세 사용자 범주 모두에 읽기 권한을 추가한다.

선지별 해설

chmod의 심볼릭 모드는 '대상·연산자·권한' 순으로 읽는다. +는 지정한 권한을 추가하고, -는 지정한 권한을 제거한다.

① X: u는 파일 소유자, w는 쓰기 권한을 뜻한다. -는 권한을 제거하는 연산자이므로 chmod u-w는 소유자의 쓰기 권한을 **제거**한다. 소유자에게 쓰기 권한을 추가하려면 chmod u+w를 사용한다.

② X: g는 파일의 소유 그룹을 뜻하며, +wx는 쓰기와 실행 권한을 추가한다는 의미이다. 따라서 chmod g+wx는 **그룹에만** 쓰기와 실행 권한을 추가한다. 그룹과 기타 사용자 모두에게 추가하려면 chmod go+wx를 사용한다.

③ O: a는 u·g·o를 모두 포함하여 소유자·그룹·기타 사용자 전체를 지정한다. +는 권한 추가, r은 읽기 권한이므로 chmod a+r는 **세 사용자 범주 모두에 읽기 권한을 추가**한다.

④ X: o는 기타 사용자, w는 쓰기 권한을 뜻한다. chmod o-w의 -는 권한 제거를 나타내므로 기타 사용자의 쓰기 권한을 **제거**한다. 기타 사용자에게 쓰기 권한을 추가하려면 chmod o+w를 사용한다.

NoteBase

문 5. 정보가 안전한 정도를 평가하는 TCSEC(Trusted Computer System Evaluation Criteria)의 보안등급 중에서 검증된 설계(Verified Design)를 의미하는 보안등급은?

① A 등급
② B 등급
③ C 등급
④ D 등급

정답 1번

간단한 해설

'검증된 설계(Verified Design)'는 **A 등급에 속하는 세부 등급 A1**의 명칭이다.

공통 해설

TCSEC에서 A는 검증된 보호(Verified Protection)를 나타내는 상위 구분이며, 그 안의 **A1이 검증된 설계(Verified Design)**에 해당한다. A1은 보안 기능이 존재하는지를 확인하는 데 그치지 않고, 정형 명세와 검증 기법을 이용하여 설계가 보안정책에 부합하는지를 검증하는 등급이다. 이 문항은 A1 같은 세부 등급 대신 A·B·C·D 중에서 고르도록 했으므로, A1을 포함하는 A 등급으로 대응시킨다.

NoteBase

문 6. 다음에서 설명하는 공격 기술은?

암호 장비의 동작 과정 중에 획득 가능한 연산시간, 전력 소모량, 전자기파 방사량 등의 정보를 활용하여 암호 알고리즘의 비밀 정보를 찾아내는 기술

① 차분 암호 분석 공격(Differential Cryptanalysis Attack)

② 중간자 공격(Man-In-The-Middle Attack)

③ 부채널 공격(Side-Channel Attack)

④ 재전송 공격(Replay Attack)

정답 3번

간단한 해설

연산시간·전력 소모량·전자기파 방사량처럼 암호 장비가 동작하면서 드러내는 **부수적 정보**로 비밀 정보를 알아내는 방식이 **부채널 공격**이다.

공통 해설

부채널 공격(Side-Channel Attack)은 암호 장비의 구현·동작 과정에서 외부로 드러나는 **부수적 정보와 비밀 정보 사이의 관계**를 분석하는 공격이다. 지문에 제시된 연산시간, 전력 소모량, 전자기파 방사량은 장비가 암호 연산을 수행하면서 관측될 수 있는 정보이므로, 이를 이용해 비밀 정보를 추정하는 기술은 부채널 공격에 해당한다.

예를 들어 비밀키를 처리하는 방식에 따라 전력 소모에 차이가 나타나는 구현에서는, 측정한 전력 소모의 패턴을 분석하여 키 정보를 추정할 수 있다. 이처럼 장비의 동작 특성이 비밀 정보를 알아내는 단서가 된다는 점이 핵심이다.

NoteBase

문 7. DoS(Denial of Service) 공격의 대응 방법에 대한 설명으로 ㉠, ㉡에 들어갈 용어는?

◯ 다른 네트워크로부터 들어오는 IP broadcast 패킷을 허용하지 않으면 자신의 네트워크가 (㉠) 공격의 중간 매개지로 쓰이는 것을 막을 수 있다.
◯ 다른 네트워크로부터 들어오는 패킷 중에 출발지 주소가 내부 IP 주소인 패킷을 차단하면 (㉡) 공격을 막을 수 있다.

① ㉠: Smurf, ㉡: Land
② ㉠: Smurf, ㉡: Ping of Death
③ ㉠: Ping of Death, ㉡: Land
④ ㉠: Ping of Death, ㉡: Smurf

정답 1번

간단한 해설

Smurf는 **브로드캐스트를 이용해 여러 호스트의 응답을 피해자에게 집중**시키므로, 외부에서 들어오는 브로드캐스트 패킷을 차단하면 중간 매개지로 악용되는 것을 막을 수 있다. Land는 **출발지와 목적지를 피해 호스트 자신으로 위조**하므로, 외부에서 유입되면서 내부 IP 주소를 출발지로 쓰는 패킷을 차단하는 방식으로 대응한다.

빈칸별 해설

㉠ Smurf: 공격자는 ICMP Echo Request의 출발지 IP 주소를 피해자의 주소로 위조하고, 이를 다른 네트워크의 브로드캐스트 주소로 보낸다. 해당 네트워크의 여러 호스트가 응답하면 그 응답이 피해자에게 몰린다. 따라서 외부에서 들어오는 **지향성 브로드캐스트 패킷을 차단**하면 자신의 네트워크가 응답을 증폭하는 중간 매개지로 쓰이는 것을 막을 수 있다. Ping of Death는 과도한 크기의 IP 패킷을 단편화해 보내고 재조립 과정의 취약점을 악용하는 공격으로, 브로드캐스트를 이용한 응답 증폭과 구별된다.

㉡ Land: 출발지와 목적지의 IP 주소 및 포트 번호를 각각 같게 만든 TCP SYN 패킷을 피해 호스트에 보내, 이를 처리하는 취약한 시스템에 장애를 일으킨다. 피해 호스트가 내부 네트워크에 있다면 이 패킷의 출발지 IP 주소도 그 내부 호스트의 주소이다. 따라서 경계에서 **외부로부터 유입되면서 내부 IP 주소를 출발지로 표시한 패킷**을 차단하면, 외부 공격자가 이러한 위조 패킷을 내부 피해 호스트에 전달하는 것을 막을 수 있다.

㉠은 Smurf, ㉡은 Land이므로 ①의 조합에 해당한다.

NoteBase

문 8. 「전자서명법」상 용어의 정의로 옳지 않은 것은?

① '전자서명'이라 함은 서명자를 확인하고 서명자가 당해 전자문서에 서명을 하였음을 나타내는 데 이용하기 위하여 당해 전자문서에 첨부되거나 논리적으로 결합된 전자적 형태의 정보를 말한다.

② '인증서'라 함은 전자서명생성정보가 가입자에게 유일하게 속한다는 사실 등을 확인하고 이를 증명하는 전자적 정보를 말한다.

③ '서명자'라 함은 전자서명검증정보를 보유하고 자신이 직접 또는 타인을 대리하여 서명을 하는 자를 말한다.

④ '전자서명생성정보'라 함은 전자서명을 생성하기 위하여 이용하는 전자적 정보를 말한다.

정답 3번

간단한 해설

구 「전자서명법」에서 서명자는 **전자서명생성정보를 보유**하고 자신이 직접 또는 타인을 대리하여 서명하는 자이다. ③의 '전자서명검증정보'는 서명을 만드는 정보가 아니라 이미 생성된 서명을 검증하는 데 쓰는 정보이다.

선지별 해설

① O: 구 「전자서명법」 제2조제2호의 전자서명은 서명자를 확인하고 해당 전자문서에 서명했다는 사실을 나타내는 전자적 정보이다. 전자문서에 직접 첨부되는 경우뿐 아니라 **논리적으로 결합된 경우도 포함**하므로, 선지의 정의와 일치한다.

② O: 구 「전자서명법」 제2조제7호의 인증서는 전자서명생성정보가 가입자에게 유일하게 속한다는 사실 등을 확인하고 증명하는 전자적 정보이다. 인증이 이를 확인·증명하는 행위라면, 인증서는 그 사실을 증명하는 **전자적 정보**라는 점에서 구별된다.

③ X: 구 「전자서명법」 제2조제12호의 서명자는 **전자서명생성정보를 보유**하고 자신이 직접 또는 타인을 대리하여 서명을 하는 자이다. 따라서 '전자서명검증정보를 보유'를 '전자서명생성정보를 보유'로 고쳐야 한다. 생성정보는 서명을 만드는 데, 검증정보는 이미 생성된 서명을 검증하는 데 사용되므로 두 정보의 역할이 다르다.

④ O: 구 「전자서명법」 제2조제4호의 전자서명생성정보는 **전자서명을 생성하는 데 이용하는 정보**이다. 전자서명 자체가 서명 사실을 나타내는 결과라면, 생성정보는 그 서명을 만들어 내는 데 쓰이는 정보이므로 선지의 정의와 일치한다.

NoteBase

문 9. 「전자정부 SW 개발·운영자를 위한 소프트웨어 개발보안 가이드」상 분석·설계 단계 보안요구항목과 구현 단계 보안약점을 연결한 것으로 옳지 않은 것은?

① 분석·설계 단계 보안요구항목: DBMS 조회 및 결과 검증, 구현 단계 보안약점: SQL 삽입

② 분석·설계 단계 보안요구항목: 디렉터리 서비스 조회 및 결과 검증, 구현 단계 보안약점: LDAP 삽입

③ 분석·설계 단계 보안요구항목: 웹서비스 요청 및 결과 검증, 구현 단계 보안약점: 크로스사이트 스크립트

④ 분석·설계 단계 보안요구항목: 보안기능 동작에 사용되는 입력값 검증, 구현 단계 보안약점: 솔트 없이 일방향 해시함수 사용

정답 4번

간단한 해설

④의 '솔트 없이 일방향 해시함수 사용'은 보안요구항목 중 **암호연산**에 대응한다. '보안기능 동작에 사용되는 입력값 검증'은 인증·권한 결정 등에 쓰이는 외부 입력값이 조작되었는지를 검증하는 항목이다.

선지별 해설

① O: 'DBMS 조회 및 결과 검증'은 SQL 질의문 생성에 쓰이는 입력값과 조회결과의 검증방법을 설계하는 항목이다. 검증되지 않은 입력이 SQL 구문으로 해석되면 질의문이 변조되어 정보의 무단 조회나 변경이 가능해지므로, **SQL 삽입**과 연결된다.

② O: '디렉터리 서비스 조회 및 결과 검증'은 LDAP 등의 디렉터리 서비스를 조회할 때 입력값과 조회결과를 검증하도록 설계하는 항목이다. 외부 입력값으로 **LDAP 검색 필터가 조작**되면 공격자가 의도한 조회가 수행될 수 있으므로 LDAP 삽입과 연결된다.

③ O: '웹서비스 요청 및 결과 검증'은 게시판 등의 요청과 응답에 포함되는 데이터를 검증하도록 설계하는 항목이다. 검증되지 않은 입력이 웹 페이지에 포함되면 사용자의 브라우저에서 악성 스크립트가 실행될 수 있으므로, **크로스사이트 스크립트(XSS)**와 연결된다. 응답 페이지에 넣는 데이터에 적절한 인코딩이나 필터링을 적용하는 것이 이에 해당한다.

④ X: '보안기능 동작에 사용되는 입력값 검증'에 대응하는 약점은 '보안기능 결정에 사용되는 부적절한 입력값'이다. 예를 들어 사용자가 수정할 수 있는 쿠키의 권한값을 서버가 검증 없이 신뢰하면 권한 상승이 발생할 수 있다. '솔트 없이 일방향 해시함수 사용'에 대응하는 보안요구항목은 **암호연산**이다. 비밀번호를 해시할 때 솔트를 함께 사용하도록 설계하여, 미리 계산해 둔 해시값을 이용한 비밀번호 추측 공격을 어렵게 해야 한다.

NoteBase

문 10. 개인정보 보호법령상 영업양도 등에 따른 개인정보의 이전 제한에 대한 내용으로 옳지 않은 것은?

① 영업양수자등은 영업의 양도·합병 등으로 개인정보를 이전받은 경우에는 이전 당시의 본래 목적으로만 개인정보를 이용하거나 제3자에게 제공할 수 있다.

② 영업양수자등이 과실 없이 서면 등의 방법으로 개인정보를 이전받은 사실 등을 정보주체에게 알릴 수 없는 경우에는 해당 사항을 인터넷 홈페이지에 10일 이상 게재하여야 한다.

③ 개인정보처리자는 영업의 전부 또는 일부의 양도·합병 등으로 개인정보를 다른 사람에게 이전하는 경우에는 미리 개인정보를 이전하려는 사실 등을 서면 등의 방법에 따라 해당 정보주체에게 알려야 한다.

④ 영업양수자등은 개인정보를 이전받았을 때에는 지체 없이 그 사실을 서면 등의 방법에 따라 정보주체에게 알려야 한다. 다만, 개인정보처리자가 「개인정보 보호법」 제27조제1항에 따라 그 이전 사실을 이미 알린 경우에는 그러하지 아니하다.

정답 2번

간단한 해설

②의 홈페이지 게재 특례는 개인정보를 이전하려는 **영업양도자등**에 관한 규정이며, 게재기간은 10일이 아니라 **30일 이상**이다.

선지별 해설

① O: 「개인정보 보호법」 제27조제3항은 영업양수자등의 개인정보 이용·제공 범위를 **이전 당시의 본래 목적**으로 제한한다. 영업을 넘겨받았다는 이유만으로 이전받은 개인정보를 새로운 목적에 자유롭게 이용하거나 제3자에게 제공할 수 있는 것은 아니다.

② X: 「개인정보 보호법 시행령」 제29조제2항의 홈페이지 게재 특례는 개인정보를 이전하려는 **영업양도자등**에 관한 규정이다. 영업양도자등이 과실 없이 서면등의 방법으로 필요한 사항을 알릴 수 없을 때에는 홈페이지에 **30일 이상** 게재하여야 한다. 따라서 선지의 '영업양수자등'과 '10일 이상'을 각각 '영업양도자등'과 '30일 이상'으로 고쳐야 한다.

③ O: 「개인정보 보호법」 제27조제1항에 따라 개인정보를 다른 사람에게 넘기는 개인정보처리자는 **이전 전에 미리** 정보주체에게 알려야 한다. 통지할 내용에는 이전 예정 사실뿐 아니라 이전받는 자의 성명·주소·연락처, 이전을 원하지 않을 때 취할 수 있는 방법과 절차가 포함된다. 통지방법은 같은 법 시행령 제29조제1항에 따른 서면등의 방법이다.

④ O: 「개인정보 보호법」 제27조제2항은 영업양수자등에게 이전받은 사실을 **지체 없이 통지할 의무**를 부과한다. 통지에는 시행령 제29조제1항에 따른 서면등의 방법을 사용한다. 다만, 개인정보를 넘긴 개인정보처리자가 법 제27조제1항에 따라 이미 통지했다면 영업양수자등이 같은 사실을 다시 알릴 의무는 없다.

NoteBase

문 11. 대칭키 암호 알고리즘에 대한 설명으로 옳은 것만을 모두 고르면?

ㄱ. AES는 128/192/256 비트 키 길이를 지원한다.
ㄴ. DES는 16라운드 Feistel 구조를 가진다.
ㄷ. ARIA는 128/192/256 비트 키 길이를 지원한다.
ㄹ. SEED는 16라운드 SPN(Substitution Permutation Network) 구조를 가진다.

① ㄱ, ㄹ
② ㄴ, ㄷ
③ ㄱ, ㄴ, ㄷ
④ ㄱ, ㄴ, ㄹ

정답 3번

간단한 해설

ㄹ의 SEED는 16라운드이지만, 전체 암호 구조는 SPN이 아니라 **Feistel 구조**이다. 라운드 수와 암호 구조는 구별해야 한다.

보기별 해설

ㄱ. O: AES는 **128·192·256비트 키**를 지원한다. 키 길이는 암호화에 사용하는 비밀키의 크기이고, 블록 길이는 한 번에 처리하는 데이터의 크기이다. AES의 블록 길이는 세 키 길이 모두에서 128비트로 일정하다.

ㄴ. O: DES는 **16라운드 Feistel 구조**를 사용한다. 64비트 데이터 블록을 두 32비트 부분으로 나누고, 한쪽에 라운드 함수를 적용한 결과를 다른 쪽과 XOR하는 연산을 반복한다.

ㄷ. O: ARIA는 AES와 마찬가지로 **128·192·256비트 키**를 지원한다. ARIA의 블록 길이 역시 128비트이므로, 키가 192비트나 256비트라고 해서 처리하는 데이터 블록도 그 크기로 늘어나는 것은 아니다.

ㄹ. X: SEED는 128비트 데이터 블록을 두 64비트 부분으로 나누어 처리하는 **16라운드 Feistel 구조**이다. 따라서 '16라운드'는 맞지만 'SPN 구조'는 'Feistel 구조'로 고쳐야 한다. SPN은 데이터에 치환과 순열에 해당하는 변환을 반복하는 구조이며, Feistel처럼 두 부분 사이의 라운드 함수 결과 결합을 기본 틀로 삼는 구조와 구별된다.

옳은 보기는 ㄱ, ㄴ, ㄷ이며, 이를 모두 포함한 조합은 ③이다.

NoteBase

문 12. 다음에서 설명하는 프로토콜은?

◯ 무선랜 통신을 암호화하는 프로토콜로서 IEEE 802.11 표준에 정의되었다.
◯ 암호화를 위해 RC4 알고리즘을 사용한다.

① AH(Authentication Header)
② SSH(Secure SHell)
③ WAP(Wireless Application Protocol)
④ WEP(Wired Equivalent Privacy)

정답 4번

간단한 해설

IEEE 802.11 무선랜에서 데이터 암호화에 **RC4**를 사용하는 보안 방식은 **WEP**이다. 무선랜 암호화라는 적용 대상과 RC4라는 암호 알고리즘을 함께 연결하면 된다.

공통 해설

WEP(Wired Equivalent Privacy)는 **IEEE 802.11 무선랜의 데이터 기밀성**을 제공하기 위해 정의된 보안 방식이다. 기밀성은 전송 내용을 허가받지 않은 사람이 알아볼 수 없도록 보호하는 성질이다. WEP는 송신 측과 수신 측이 공유하는 비밀키를 바탕으로 RC4를 사용한다. RC4로 생성한 키스트림을 원문 데이터와 XOR하여 암호화하고, 수신 측은 같은 키스트림으로 원문을 복원한다. 따라서 지문의 무선랜 암호화와 RC4 사용이라는 두 특징에 해당하는 프로토콜은 WEP이다.

NoteBase

문 13. 기밀성을 제공하는 암호 기술이 아닌 것은?

① RSA

② SHA-1

③ ECC

④ IDEA

정답 2번

간단한 해설

SHA-1은 데이터를 암호화하는 기술이 아니라 **고정 길이의 요약값을 만드는 해시 함수**이다. 복호화하여 원문을 전달하는 암호화 기능이 없으므로 기밀성을 제공하지 않는다.

공통 해설

기밀성은 허가받지 않은 사람이 정보의 내용을 알 수 없도록 하는 성질이다. 이를 위한 암호화는 평문을 암호문으로 바꾸고, 허가받은 수신자는 **적절한 키로 복호화하여 원문을 복원**하도록 한다. RSA와 ECC는 공개키 기반 암호 기술이고 IDEA는 대칭키 암호 기술로, 모두 암호화에 활용하여 정보의 내용을 보호할 수 있다.

SHA-1은 입력 데이터로부터 고정 길이의 해시값을 계산하는 해시 함수이다. 해시값은 복호화할 암호문이 아니며, **키로 해시값을 복호화하여 원문을 복원하는 절차가 없다**. 따라서 SHA-1으로 요약값을 만드는 것만으로는 원문의 내용을 숨기는 기밀성이 제공되지 않는다.

NoteBase

문 14. SSL 프로토콜에 대한 설명으로 옳지 않은 것은?

① 전송계층과 네트워크계층 사이에서 동작한다.

② 인증, 기밀성, 무결성 서비스를 제공한다.

③ Handshake Protocol은 보안 속성 협상을 담당한다.

④ Record Protocol은 메시지 압축 및 암호화를 담당한다.

정답 1번

간단한 해설

SSL은 **응용계층과 전송계층 사이**에서 동작하며, TCP가 제공하는 신뢰성 있는 전송을 이용해 응용계층 데이터를 보호한다. 전송계층과 네트워크계층 사이에서 동작한다는 설명은 계층 위치를 잘못 짚은 것이다.

선지별 해설

① X: SSL은 **응용계층과 전송계층 사이**에 위치한다. 응용 프로그램이 보낸 데이터를 SSL이 보호한 뒤 TCP로 전달하므로, 전송계층과 네트워크계층 사이에서 동작한다는 표현은 잘못이다.

② O: SSL은 인증으로 통신 상대의 신원을 확인하고, 암호화로 데이터의 기밀성을 보호하며, 메시지 인증 코드(MAC)로 전송 중 데이터의 변경 여부를 확인하여 무결성을 제공한다. 이때 **클라이언트 인증은 선택적**이므로 모든 연결에서 양쪽이 반드시 인증하는 것은 아니다.

③ O: Handshake Protocol은 클라이언트와 서버가 통신에 사용할 **암호 알고리즘과 압축 방식 등 보안 속성을 협상**하도록 한다. 또한 인증과 키 교환을 수행하여 이후 데이터를 보호하는 데 필요한 보안 매개변수를 마련한다.

④ O: Record Protocol은 상위 계층의 데이터를 적절한 크기로 나누고, 협상된 압축 방식을 적용한 뒤 MAC을 붙이고 암호화하여 전달한다. 따라서 **메시지 압축과 암호화**는 Record Protocol의 역할이다. 다만 압축을 하지 않는 방식이 선택되면 실제 데이터 압축은 수행하지 않는다.

NoteBase

문 15. DSA(Digital Signature Algorithm)에 대한 설명으로 옳지 않은 것은?

① 기밀성과 부인방지를 동시에 보장한다.

② NIST에서 발표한 전자서명 표준 알고리즘이다.

③ 전자서명의 생성 및 검증 과정에 해시함수가 사용된다.

④ 유한체상의 이산대수문제의 어려움에 그 안전성의 기반을 둔다.

정답 1번

간단한 해설

DSA는 전자서명을 통해 무결성·서명자 인증·부인방지를 제공하지만, 메시지 내용을 암호화하지 않으므로 **기밀성을 보장하지 않는다**. 기밀성이 필요하면 별도의 암호화를 적용해야 한다.

선지별 해설

① X: DSA는 서명자의 개인키로 서명을 생성하고 대응하는 공개키로 검증하는 전자서명 알고리즘이다. 메시지의 변조 여부와 서명자를 확인하고, 서명자가 나중에 서명 사실을 부인하기 어렵게 하는 근거를 제공한다. 그러나 **메시지 내용을 숨기는 암호화 기능은 제공하지 않는다**. 따라서 부인방지는 제공하지만 기밀성까지 동시에 보장한다는 설명은 잘못이며, 기밀성을 위해서는 별도의 암호화가 필요하다.

② O: DSA는 미국 국립표준기술연구소(NIST)가 발표한 **전자서명 표준 DSS**에 포함된 알고리즘이다. 예를 들어 FIPS 186-4는 DSA를 이용한 서명 생성과 검증 방법을 규정했다. DSS는 표준의 명칭이고 DSA는 그 표준에 포함된 알고리즘의 명칭이다.

③ O: DSA에서는 서명할 메시지에 해시함수를 적용하여 얻은 해시값을 서명 계산에 사용한다. 검증할 때도 수신한 메시지에 **동일한 해시함수**를 적용하고, 그 결과와 서명·공개키를 이용해 서명의 유효성을 확인한다. 따라서 생성과 검증 모두에 해시함수가 사용된다.

④ O: DSA의 공개키는 유한체의 곱셈군에 속하는 부분군에서 개인키를 지수로 하는 거듭제곱 연산으로 만들어진다. 이 공개키와 공개된 매개변수로부터 개인키에 해당하는 지수를 알아내는 것이 **이산대수문제**이다. 적절한 매개변수 아래에서 이 문제를 풀기 어렵다는 점이 DSA의 안전성 기반이다.

NoteBase

문 16. 무의미한 코드를 삽입하고 프로그램 실행 순서를 섞는 등 악성코드 분석가의 작업을 방해하는 기술은?

① 디스어셈블(Disassemble)

② 난독화(Obfuscation)

③ 디버깅(Debugging)

④ 언패킹(Unpacking)

정답 2번

간단한 해설

무의미한 코드를 삽입하거나 실행 흐름을 복잡하게 바꾸어 분석을 어렵게 하는 기술은 **난독화**이다. 프로그램의 기능은 유지하면서 내부 동작을 쉽게 파악하지 못하도록 만든다.

공통 해설

난독화(Obfuscation)는 **프로그램의 기능을 유지하면서 코드의 이해와 분석을 어렵게 만드는** 기술이다. 문항의 무의미한 코드 삽입은 실제 기능에 필요 없는 코드를 섞어 분석가가 중요한 동작을 가려내기 어렵게 하는 방식이다. 실행 순서를 섞는 방식도 필요한 동작과 결과를 유지하면서 분기 등으로 제어 흐름을 복잡하게 만들어, 다음에 어떤 코드가 실행되는지 추적하기 어렵게 한다. 이처럼 코드 자체를 변형하여 악성코드 분석을 방해한다는 설명은 난독화에 해당한다.

NoteBase

문 17. 윈도우즈용 네트워크 및 시스템 관리 명령어에 대한 설명으로 옳은 것은?

① ping - 원격 시스템에 대한 경로 및 물리 주소 정보를 제공한다.

② arp - IP 주소에서 물리 주소로의 변환 정보를 제공한다.

③ tracert - IP 주소, 물리 주소 및 네트워크 인터페이스 정보를 제공한다.

④ ipconfig - 원격 시스템의 동작 여부 및 RTT(Round Trip Time) 정보를 제공한다.

정답 2번

간단한 해설

arp는 **IPv4 주소와 물리 주소(MAC 주소)의 대응 정보**를 관리·조회하는 명령어이다. ARP 캐시를 조회하면 저장된 IP 주소에 대응하는 MAC 주소를 확인할 수 있다.

선지별 해설

① X: ping은 ICMP 에코 요청을 보내 원격 호스트의 **응답 여부와 왕복 시간(RTT)**을 확인한다. 목적지까지의 경로를 추적하는 명령어는 tracert이며, IP 주소와 물리 주소의 대응 정보는 arp로 확인한다.

② O: arp는 **IPv4 주소와 MAC 주소의 대응 정보**를 담은 ARP 캐시를 조회·관리한다. 예를 들어 arp -a를 실행하면 캐시에 저장된 IP 주소와 그에 대응하는 물리 주소를 확인할 수 있으므로, 선지의 설명과 일치한다.

③ X: tracert는 목적지까지 패킷이 거치는 **중간 라우터의 경로**를 추적한다. 로컬 컴퓨터의 IP 주소와 네트워크 인터페이스별 설정을 확인하는 명령어는 ipconfig이며, ipconfig /all을 사용하면 물리 주소도 함께 확인할 수 있다.

④ X: ipconfig는 로컬 컴퓨터의 **네트워크 인터페이스별 IP 설정**을 표시한다. IP 주소, 서브넷 마스크, 기본 게이트웨이 등을 확인하는 데 쓰며, 원격 호스트의 응답 여부와 RTT를 확인하는 명령어는 ping이다.

NoteBase

문 18. 정보자산에 대한 위험분석에서 사용하는 ALE(Annualized Loss Expectancy, 연간예상손실액), SLE(Single Loss Expectancy, 1회손실예상액), ARO(Annualized Rate of Occurrence, 연간발생빈도) 사이의 관계로 옳은 것은?

① ALE = SLE + ARO

② ALE = SLE × ARO

③ SLE = ALE + ARO

④ SLE = ALE × ARO

정답 2번

간단한 해설

연간예상손실액은 **1회손실예상액에 연간발생빈도를 곱한 값**이다. 따라서 세 값의 관계는 ALE = SLE · ARO 이다.

공통 해설

SLE는 위험이 한 번 발생했을 때의 예상 손실액이고, ARO는 그 위험이 1년 동안 발생할 것으로 예상되는 횟수이다. ALE는 그 위험으로 인한 연간 예상 손실액이므로, **한 번의 손실액에 연간 발생 횟수를 곱하여** 구한다. 즉, ALE = SLE · ARO이다.

예를 들어 1회손실예상액이 100만 원이고 연간발생빈도가 2회라면, 연간예상손실액은 100만 원 × 2 = 200만 원이다. 이는 해당 위험으로 1년에 평균적으로 예상하는 손실액을 뜻한다.

손실액과 발생빈도는 단위가 다르므로 둘을 더하는 식은 성립하지 않는다. 반대로 연간예상손실액에서 1회손실예상액을 구할 때에는, ARO가 0보다 크면 **연간발생빈도로 나누어야** 한다. 이때 관계식은 $\mathrm{SLE} = \frac{\mathrm{ALE}}{\mathrm{ARO}}$ 이며, ALE에 ARO를 다시 곱하는 식과 구별된다.

NoteBase

문 19. 「개인정보 보호법」상 개인정보 보호 원칙으로 옳지 않은 것은?

① 개인정보처리자는 개인정보의 처리 목적을 명확하게 하여야 하고 그 목적에 필요한 범위에서 최소한의 개인정보만을 적법하고 정당하게 수집하여야 한다.

② 개인정보처리자는 개인정보의 처리 목적에 필요한 범위에서 적합하게 개인정보를 처리하여야 하며, 그 목적 외의 용도로 활용하여서는 아니 된다.

③ 개인정보처리자는 개인정보의 익명처리가 가능한 경우에는 익명에 의하여 처리될 수 있도록 하여야 한다.

④ 개인정보처리자는 개인정보 처리방침 등 개인정보의 처리에 관한 사항을 비밀로 하여야 한다.

정답 4번

간단한 해설

④의 '비밀로 하여야 한다'는 **'공개하여야 한다'**로 고쳐야 한다. 개인정보 처리방침 등 처리에 관한 사항을 공개하여 정보주체가 자신의 개인정보 처리 내용을 알고 권리를 행사할 수 있도록 해야 한다.

선지별 해설

① O: 「개인정보 보호법」 제3조제1항은 처리 목적을 명확히 하고, 그 목적에 필요한 **최소한의 개인정보만** 적법하고 정당하게 수집하도록 한다. 수집 목적이 분명하더라도 그 목적에 필요하지 않은 정보까지 수집해서는 안 된다.

② O: 제3조제2항은 개인정보를 **처리 목적에 필요한 범위에서 적합하게 처리**하고, 그 목적 외의 용도로 활용하지 않도록 한다. 적법하게 수집한 정보라도 수집했다는 이유만으로 다른 용도에 자유롭게 사용할 수 있는 것은 아니다.

③ O: 제3조제7항은 익명처리가 가능한 경우 익명으로 처리하도록 하는 원칙을 둔다. 익명처리는 개인을 알아볼 수 없도록 처리하는 것으로, **개인을 식별하지 않고도 수집 목적을 달성할 수 있다면** 익명으로 처리하여 사생활 침해 위험을 줄여야 한다.

④ X: 제3조제5항에 따라 개인정보 처리방침 등 개인정보의 처리에 관한 사항은 **공개하여야 한다**. 공개 대상은 개인정보를 어떻게 처리하는지에 관한 방침과 사항이며, 개인의 개인정보 자체를 누구나 보도록 공개한다는 뜻은 아니다. 처리의 투명성을 확보하고 열람청구권 등 정보주체의 권리를 보장해야 하므로, 이를 비밀로 해야 한다는 설명은 반대이다.

NoteBase

문 20. 다음에서 설명하는 블록암호 운용 모드는?

◯ 암·복호화 모두 병렬 처리가 가능하다.
◯ 블록 암호 알고리즘의 암호화 로직만 사용한다.
◯ 암호문의 한 비트 오류는 복호화되는 평문의 한 비트에만 영향을 준다.

① ECB
② CBC
③ CFB
④ CTR

정답 4번

간단한 해설

CTR은 **카운터를 독립적으로 암호화한 값**을 데이터와 XOR한다. 이 구조로 암·복호화 모두 병렬 처리가 가능하고 암호화 로직만 사용하며, 암호문 한 비트 오류는 대응하는 평문 한 비트에만 영향을 준다.

공통 해설

CTR(카운터 모드)은 블록마다 서로 다른 카운터 값을 암호화해 키 스트림을 만들고, 이를 평문과 XOR해 암호문을 얻는 방식이다. 복호화할 때도 같은 키와 대응하는 카운터를 암호화하여 동일한 키 스트림을 만든 뒤 암호문과 XOR한다. 같은 값을 두 번 XOR하면 원래 값으로 돌아오므로, 블록 암호의 복호화 로직 없이 **암호화 로직만으로 암·복호화**를 수행한다.

각 블록의 키 스트림은 해당 카운터와 키로 결정되며 이전 블록의 처리 결과를 기다릴 필요가 없다. 따라서 여러 카운터의 암호화와 각 데이터 블록의 XOR 연산을 독립적으로 수행할 수 있어 **암호화와 복호화 모두 병렬 처리**가 가능하다.

전송 중 암호문의 한 비트가 뒤집혀도 카운터와 키가 그대로라면 복호화에 쓰는 키 스트림은 바뀌지 않는다. XOR 결과에서는 그 위치의 평문 비트만 뒤집히고, 다른 비트나 다른 블록에는 오류가 전파되지 않는다. 따라서 지문의 세 특성은 모두 CTR의 작동 구조에서 나온다.

NoteBase